IN THE CLAIMS

This is a complete and current listing of the claims, marked with status identifiers in parentheses. The following listing of claims will replace all prior versions and listings of claims in the application.

1. – 16. (Cancelled).

17. (New) Data exchange method between two devices locally connected to one another, especially between a security module and a receiver, the first device comprising at least one first encrypting key of a pair of asymmetric keys and the second device comprising at least the second encrypting key of said pair of asymmetric keys, these keys being previously initialised in the first and second device, this method comprising:

- generating, at least one first random number in the first device,
- generating, at least one second random number in the second device,
- encrypting said first random number by said first encrypting key,
- encrypting said second random number by said second encrypting key,
- transmitting said first encrypted random number to the second device,
- transmitting said second encrypted random number to the first device,
- decrypting the first encrypted random number in said second device,
- decrypting the second encrypted random number in said first device,
- combining said random numbers generated by one of the devices and received by the other device to generate a session key,
- and using the session key to encrypt and decrypt all or part of the exchanged data between the first and second device.

18. (New) Data exchange method according to claim 17, wherein random number, generated by the first device and decrypted by the second device

- is encrypted by said second device by means of said second encrypting key,
- is transmitted in a encrypted form to said first device,
- is decrypted in this first device by means of the first encrypting key and

- is compared to said random number generated by the first device,

and wherein the data transfer is stopped if the compared random numbers are not identical.

19. (New) Data exchange method according to claim 17, wherein the random number, generated by the second device and decrypted by the first device

- is encrypted by said first device by means of said first encrypting key,
- is transmitted in a encrypted form to said second device,
- is decrypted in this second device by means of the second encrypting key and
- is compared to said random number generated by the second device,

and wherein the data transfer is stopped if the compared random numbers are not identical.

20. (New) Data exchange method according to claim 17, in which said first device and said second device contain a symmetric encrypting key, wherein the random numbers are combined with said symmetric key to generate a session key.

21. (New) Data exchange method according to claim 17, wherein the combination of said random numbers is a concatenation.

22. (New) Data exchange method according to claim 20, wherein the combination of said random numbers is a concatenation.

23. (New) Data exchange method according to claim 17, wherein the session key is regenerated in function of a determined parameter of use.

24. (New) Data exchange method according to claim 23, wherein the determined parameter of use is the duration of use.

25. (New) Data exchange method according to claim 17, wherein at least one of the two devices measures at least one representative physical parameter of the communication, such as the line impedance and/or the electric consumption, wherein one compares the values measured to the reference

values, and wherein one acts on the data exchange when the measured parameters differ from the reference values more than a threshold value.

26. (New) Data exchange method according to claim 25, wherein one acts by stopping the data exchange between the two devices.

27. (New) Data exchange method according to claim 25, wherein the session key is regenerated in function of a determined parameter of use and wherein the determined parameter of use is the representative physical parameter of the communication.

28. (New) Data exchange method according to claim 17, wherein

- at least one of the devices generates at least one supplementary random number,
- this supplementary random number is encrypted by said first encrypting key,
- this supplementary encrypted random number is transmitted to the second device,
- this transmitted encrypted supplementary random number is decrypted in this second device,
- the decrypted supplementary random number is encrypted by said second encrypting key,
- the supplementary encrypted random number is transmitted to the first device,
- the supplementary random number decrypted in the first device is compared to the initial supplementary random number generated in said first device,
- the information exchange is interrupted if the comparison indicates that the two compared numbers are not identical.

29. (New) Data exchange method according to claim 17, wherein

- at least one of the devices determines at least one predefined fixed number memorized in the two devices,
- this predefined fixed number is encrypted by said first encrypting key,

- this predefined fixed encrypted number is transmitted to the second device,
- this transmitted encrypted predefined fixed number is decrypted in this second device,
- the predefined fixed number decrypted in the second device is compared to the predefined fixed number memorized in this second device,
- the data exchange is interrupted if the comparison indicates that the two compared numbers are not identical.

30. (New) Data exchange method according to claim 28, wherein each of the numbers is encrypted separately.

31. (New) Data exchange method according to claim 29, wherein each of the numbers is encrypted separately.

32. (New) Data exchange method according to claim 28, wherein a combination of each of the numbers is encrypted.

33. (New) Data exchange method according to claim 29, wherein a combination of each of the numbers is encrypted.

34. (New) Receiver for carrying out the method according to claim 17, this receiver comprising at least one calculation unit, a read-only memory, a demultiplexer, a descrambler, a digital/analog converter, an external memory and a sound and image descrambler, wherein at least the calculation unit, the read-only memory and the descrambler are contained in a same electronic chip and wherein at least one of the encrypting keys is stored in said electronic chip.

35. (New) Receiver according to claim 34, wherein at least one of the numbers is stored in said electronic chip.